AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims

Claim 1 (Currently Amended): A digital private key protection device, comprising:

a digital key storage containing a user's digital private key;

a cryptographic engine for processing digital data and one or more digital keys;

a communications port for receiving digital data ~~including~~ from an external device, wherein the digital data includes a document ~~to be signed from an external device~~ visually setting forth obligations to which the user is to be contractually bound upon assent thereto by the user, and wherein the communications port is configured for transmitting data external of said digital private key protection device;

a trusted display for displaying said received digital data including [[a]] the document;

a user operable input connected to said cryptographic engine to indicate when operated by said user their ~~approval of said displayed received digital data including a document~~ assent to the obligations set forth in the document displayed on the trusted display such that document cannot be repudiated; wherein

said cryptographic engine is trusted to only apply said user's digital private key to sign said received digital data only if said user operable input is operated and communicate said signed data including [[a]] the document external of said digital private key protection device.

Claim 2 (Previously Presented): A digital private key protection device according to claim 1, wherein said digital key storage also contains a trusted public key and a plurality of user's public keys signed so as to be verifiable by the trusted public key; and said cryptographic engine validates signature of said user's public key with said trusted public key to determine the veracity of a said user's public key and then processes said received digital

data using said verified predetermined user's public key and causes said trusted display to indicate whether said user's private key was used to sign said received digital data.

Claim 3 (Previously Presented): A digital private key protection device according to claim 1, wherein said received digital data includes a digital certificate.

Claim 4 (Currently Amended): A digital private key protection device according to claim 1 further comprising an audit means wherein signed data is not transmitted external of said digital private key protection device until said audit means ~~audits~~ records in an audit trail a record of the ~~signing~~ validation performed by said cryptographic engine.

Claim 5 (Currently Amended): A digital private key protection device according to claim 2 further comprising an audit means wherein signed received digital data is not displayed by said trusted display until said audit means ~~audits~~ records in an audit trail a record of the ~~signing~~ validation performed by said cryptographic engine.

Claim 6 (Previously Presented): A digital private key protection device according to claim 1 wherein said digital key storage further includes said digital private key protection device's private key wherein digital data signed by said digital private key protection device after operation of said user operable input is further signed by said private key of said digital private key protection device.

Claim 7 (Currently Amended): A digital private key protection device according to claim [[6]] 25 wherein said digital key storage also includes said digital private key protection device's public key; such that when said communications port receives signed digital data from an external device which may or may not have been signed by said digital private key protection device's private key;

said cryptographic engine ~~decrypts~~ verifies said received data using said digital private key protection device's public key to verify whether said digital private key

protection device's predetermined digital private key was used to ~~encrypt~~ sign said received digital data.

Claim 8 (Currently Amended): A digital private key protection device according to claim 7 wherein said trusted display means indicates whether said digital private key protection device's private key was used to ~~encrypt~~ sign said received digital data.

Claim 9 (Currently Amended): A digital private key protection device according to claim 1 wherein the digital key storage includes a plurality of user's public keys; and

said received digital data contains information that predetermines which user's public key is used to encrypt said displayed received digital data that is transmitted external of said digital private key protection device to a predetermined user.

Claim 10 (Previously Presented): A digital private key protection device according to claim 1 wherein said cryptographic engine is trusted to decrypt received digital data using said user's digital private key and passing decrypted digital data to said trusted display for display of said received digital data.

Claim 11 (Currently Amended): A digital private key protection device according to claim 10 wherein displayed decrypted received digital data is not released external to said device unless said user operable input is operated.

Claim 12 (Previously Presented): A digital private key protection device according to claim 10 wherein said communications port cannot transmit said decrypted digital data external of said digital private key protection device.

Claim 13 (Canceled)

Claim 14 (Previously Presented): A digital private key protection device according to claim 1 wherein said digital key storage also contains a digital shared secret symmetric key wherein said cryptographic engine only applies said digital shared secret symmetric key to encrypt signed received digital data only if said user operable input means is operated and to

communicate said encrypted signed received digital data external of said digital private key protection device.

Claim 15 (Previously Presented): A digital private key protection device according to claim 1, wherein said received digital data contains an instruction which determines how said cryptographic engine should process the received digital data.

Claim 16 (Previously Presented): A digital private key protection device according to claim 1, wherein said received digital data contains an instruction which determines which protocol is used by said digital private key protection device to communicate encrypted or signed received digital data external of said digital private key protection device.

Claim 17 (Previously Presented): A digital private key protection device according to claim 1, wherein said trusted display is external to said digital private key protection device and controlled by said digital private key protection device for displaying data transmitted from said communications port in a trusted manner.

Claim 18 (Previously Presented): A digital private key protection device according to claim 1, wherein said user operable input is external to said digital private key protection device and controlled by said digital private key protection device to be actuated by said user in a predetermined manner.

Claim 19 (Previously Presented): A digital private key protection device according to claim 1, further comprising identification and authentication means actuated by said user in a predetermined manner.

Claim 20 (Previously Presented): A digital private key protection device according to claim 1 further comprising an audit means which audits the actuation of said user operable input.

Claim 21 (Previously Presented): A digital private key protection device according to claim 1, wherein the digital key storage is removable from said digital private key protection device.

Claim 22 (Currently Amended): A digital private key protection device according to claim [[6]] 25, wherein a cryptographic request is received from an external device according to a predetermined application programming interface, such that the request is performed by said digital private key protection device using the user's private or other keys as identified by the request, but excluding any private keys associated with the digital private key protection device with the result being transmitted to said external device or a predetermined destination included in said request or otherwise predetermined.

Claim 23 (Previously Presented): A digital private key protection device according to claim 22 wherein said trusted display displays a description of said cryptographic request to the user and, only if the user operates said user operable input, does said digital private key protection device carry out said cryptographic request.

Claim 24 (Previously Presented): A digital private key protection device according to claim 1, wherein the digital key storage is adapted to allow removal of the user's digital keys from the digital private key protection device.

Claim 25 (New): A digital private key protection device, comprising:

a digital key storage containing a user's digital private key;

a cryptographic engine for processing digital data and one or more digital keys;

a communications port for receiving digital data from an external device, wherein the digital data includes a document to be viewed and signed so that the document cannot be repudiated, and wherein the communications port is configured for transmitting data external of said digital private key protection device;

a trusted display for displaying said received digital data including the document;

a user operable input connected to said cryptographic engine to indicate when operated by said user their assent to the obligations set forth in the document displayed on the trusted display such that document cannot be repudiated; wherein

said cryptographic engine is trusted to only apply said user's digital private key to sign said received digital data only if said user operable input is operated and communicate said signed data including the document external of said digital private key protection device and a digital private key protection devices' private key wherein digital data signed by said digital private key protection device after operation of said user operable input is further signed by said private key of said digital private key protection device.